UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

5

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,747	10/26/2001	William H. Dixon	210818	5741

22971 7590 04/19/2006

MICROSOFT CORPORATION
ATTN: PATENT GROUP DOCKETING DEPARTMENT
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER
DERWICH, KRISTIN M

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/014,747	**Applicant(s)** DIXON ET AL.
	Examiner Kristin Derwich	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 are pending.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 16, 2006 has been entered.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

2. Claims 1, 5, 7-12 rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al, (Nessett), U.S. Patent No. 5,968,176 in view of Markam et al. (Markham), Security at the Network Edge.

As per claim 1:

Nessett substantially teaches a distributed firewall (DFW) comprising:

an authentication component for providing user authentication for connection attempts from users attempting to access the end system via a network (13:39-45);

In this instance the switch functions as an authentication component by providing user authentication protocols for servers, wherein servers function as networks, attempting to access an end system.

an access control component for providing purpose authorization for authenticated users based on rules in a connection policy associating users with purposes (12:10-11, 17-19; 16:6-10);

Wherein the NIC or modem functions as the access control component and the filtering rules function as the connection policy associating users with specific filtering rules which function as purpose authorizations.

an enforcement component for enforcing the connection policy rule for the authenticated user from whom the traffic is sent as the traffic is received (16:10-12);

Wherein the enforcement component is the Access Server.

and wherein the authentication component utilizes an aggregate of the users in the connection policy to authenticate users (16:58-67 – 17:1-3).

Nessett fails to disclose these features implemented on an end system. However, Markham dislcloses a distributed firewall architecture that pushes network security policy enforcement to the edge of the network all the way to the host, which is the end system (pg. 279, col. 2, 2nd paragraph), including connection policies (pg. 281, col. 1, 2nd paragraph, table 1) and enforcement (pg. 281, col. 2, last paragraph). Note: the distributed firewall is implemented on a NIC which is part of the end system.

As per claim 5:

Nessett and Markham substantially teach a DFW wherein the end system enforcement component utilizes Internet protocol security (IPSec) protocol to maintain security of communications from the authenticated user when the communications are within the rule in the connection policy (16:27-29).

As per claim 7:

Nessett and Markham substantially teach a DFW further comprising an end system inspection component for inspecting packets from an authenticated user (13:53-56).

Wherein the router functions as the inspection component and checking the packet's quality of service, security option data and hop count function as inspecting the packet.

As per claim 8:

Nessett and Markham substantially teach a DFW wherein the connection policy is defined in a pluggable policy component (16:6-12).

Wherein the Access Server functions as a pluggable policy component.

As per claim 9:

Nessett and Markham substantially teach a DFW wherein the pluggable policy component is downloaded from a centralized administrative policy (15:29-33).

Wherein the centralized administrative policy is the Remote PSTN and Remote Access Router.

As per claim 10:

Nessett and Markham substantially teach a DFW wherein the pluggable policy component is modifiable on the end system (17:12-14).

Wherein the Remote Access equipment includes the Access Server which functions as the pluggable policy component.

As per claim 11:

Nessett and Markham substantially teach a DFW further comprising an end system access control component through which the connection policy may be defined (7:36-38).

As per claim12:

Nessett and Markham substantially teach a DFW further comprising an end system access control component having a user interface (UI) through which the connection policy is defined (7:38-41).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Nessett and Markham because Nessett seeks to implement a system which allows for coordinated security policy across multiple layers of network systems (3:15-17). This includes in an end system NIC such as that taught by Markham (3:19-40). Therefore, the firewall capabilities described in Markham used in combination with the distributed firewall of Nessett would increase the security of a distributed firewall since Markham seeks to protect against inside attackers (pg. 279, col. 1, last paragraph).

3. Claims 2-4 rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett (U.S. 5,968,176) in view of Markham (Network Edge Security), as applied to claim 1 above and further in view of Harkins et al. (RFC 2409, The Internet Key Exchange) hereinafter referred to as Harkins.

As per claim 2:

Nessett and Markham substantially teach an authentication component utilizing IPSEC to authenticate users based on the aggregate of users in the connection policy but fails to teach users being authenticated in IKE main mode as the IPSEC protocol. However, Harkins discloses utilizing IKE in main mode to authenticate users (pg. 20, section 8, 3rd paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use IKE main mode in order to authenticate a user because this provides for perfect forward secrecy of keys and identities which would allow for better security (pg. 20, section 8, 1st and 2nd paragraph).

As per claim 3:

Nessett and Markham substantially teach an authentication component utilizing the rule in the connection policy to authenticate the user but fails to teach the authentication in IKE quick mode. However, Harkins discloses utilizing IKE quick mode to complete the authentication of a user (pg. 20, section 8, 4th paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to complete authentication in IKE quick mode because this would have provided for perfect forward secrecy of the keys and identities which would provide better security (pg. 20, section 8, 1st and 2nd paragraph).

As per claim 4:

Nessett and Markahm fail to teach an authentication component that transmits a secure notify message to the authenticated user when the user sends traffic in quick mode that exceeds an authority governed by the rule in the connection policy associated with the user. However, Harkins discloses a notify message being sent when identifiers are not acceptable based on the policy established by the client (pg. 13, 4th paragraph, lines 6-10). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to notify the user when identities exceed the policies set forth because the ensures traffic is directed to the correct tunnels when multiple tunnels exist (pg. 13, 5th paragraph, lines 1-4).

4. Claim 6 rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett (U.S. 5,968,176) in view of Markham (Network Edge Security), as applied to claim 1 above and further in view of LeBlanc (Bind Basics).

As per claim 6:

Nessett and Markham fail to teach enabling IPSec on a socket and binding it in exclusive mode. However, LeBlanc discloses a method for binding the socket in exclusive mode using SO_EXCLUSIVEADDREUSE (pg. 2, 6th paragraph, lines 1-2). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to enable IPSec on a socket binding in exclusive mode because the operating system prefers a socket bound to a specific address since this will also prevent hijacker attacks (pg. 2, 2nd paragraph, lines 2-6).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kristin Derwich

Examiner
Art Unit 2132

KMD
KMD

Gilberto

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100